An efficient identity-based broadcast signcryption scheme

Hien D.T., Tien T.N., Thu Hien T.T.
Hanoi University of Engineering and Technology, VNUH, Viet Nam; Nancy University, INRIA Nancy Grand Est Research Center, France

Abstract: It is a challenge to find out a suitable algorithm for broadcasting information securely and authentically to only target users. Many schemes based on public and symmetric key cryptography have been investigated. However, modeling an efficient scheme that provides both confidentiality and public ciphertext authenticity is still an open problem. In this paper, we present an identity-based broadcast signcryption scheme with short ciphertext size and public ciphertext authenticity. The security of this scheme is proved under computational assumptions and in the random oracle model. Experimental results are also provided and compared with several schemes in both computation and communication cost. © 2010 IEEE.

Index Keywords: Ciphertexts; Communication cost; Computational assumptions; Identity-based; Open problems; Random Oracle model; Signcryption schemes; Symmetric key cryptography; Systems engineering; Cryptography

Year: 2010
Source title: Proceedings - 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Art. No.: 5632005
Page : 209-216
Link: Scorpus Link
Correspondence Address: Hien, D. T.; Hanoi University of Engineering and Technology, VNUHViet Nam; email: hiendt@vnu.edu.vn
Conference name: 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Conference date: 7 October 2010 through 9 October 2010
Conference location: Hanoi
Conference code: 83923
ISBN: 9.78077E+12
DOI: 10.1109/KSE.2010.17
Language of Original Document: English
Abbreviated Source Title: Proceedings - 2nd International Conference on Knowledge and Systems Engineering, KSE 2010
Document Type: Conference Paper
Source: Scopus

Authors with affiliations:

- Hien, D.T., Hanoi University of Engineering and Technology, VNUH, Viet Nam
- Tien, T.N., Hanoi University of Engineering and Technology, VNUH, Viet Nam

- Thu Hien, T.T., Nancy University, INRIA Nancy Grand Est Research Center, France

References:

- Shamir, A., Identity-based cryptosystems and signature schemes (1984) In Advances in Cryptology - Crypto '84, 196, pp. 47-53
- Fiat, A., Naor, M., Broadcast encryption (1994) CRYPTO 1993, LNCS, 773, pp. 480-491
- Delerablee, C., Identity-based broadcast encryption with constant size ciphertext and priavate keys (2007) Lecture Notes in Computer Science, Springer-Verlag, 4833, pp. 200-215
- Baek, J., Safavi-Naini, R., Susilo, W., Efficient multi-receiver identity-based encryption and its application to broadcast encryption (2005) Lecture Notes in Computer Science, 3386, pp. 380-397. , Public Key Cryptography - PKC 2005 - 8th International Workshop on Theory and Practice in Public Key Cryptography
- Boneh, D., Gentry, C., Waters, B., Collusion resistant broadcast encryption with short ciphertexts and private keys (2006) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3621, pp. 258-275. , Advances in Cryptology - CRYPTO 2005 - 25th Annual International Cryptology Conference, Proceedings
- Zheng, Y., (1997) Digital Signcryption or How to Achieve Cost (Signature & Encryption) Cost (Signature) + Cost (Encryption), 1
- Mu, Y., Varadharajan, V., Distributed Signcryption (2000) LECTURE NOTES IN COMPUTER SCIENCE, (1977), pp. 155-164. , Progress in Cryptology - INDOCRYPT 2000
- Li, F., Hu, Y., Liu, S., Efficient and provably secure multi-recipient signcryption from bilinear pairings (2006) Cryptology EPrint Archive, Report 2006/238
- Ma, C.B., Ao, J., Li, J.H., How to signcrypt a message to designated group (2007) The Journal of China Universities of Posts and Telecommunications, 14 (4), pp. 57-63
- Bohio, M., Miri, A., An authenticated broadcasting scheme for wireless ad hoc network (2004) Second Annual Conference on Communication Networks and Services Research, pp. 69-74
- Duan, S., Cao, Z., Efficient and provably secure multi-receiver identity-based signcryption (2006) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4058, pp. 195-206. , Information Security and Privacy: 11th Australasian Conference, ACISP 2006, Proceedings
- Tan, C.-H., On the security of provably secure multi-receiver id-based signcryption scheme (2008) IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E91-A (7), pp. 1836-1838. , ISSN 0916-8508
- Boyen, X., Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography (2003) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2729, pp. 383-399
- Yu, Y., Yang, B., Huang, X.Y., Zhang, M.W., Efficient identity-based signcryption scheme for multiple receivers (2007) Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 4610, pp. 13-21
- Elkamchouchi, H., Abouelseoud, Y., Midscyk: An efficient provably secure multi-recipient identity-based signcryption scheme (2009) International Conference on Networking and Media Convergence 2009, pp. 70-75
- Selvi, S.S.D., Vivek, S.S., Srinivasan, R., Rangan, C.P., An efficient identity-based signcryption scheme for multiple receivers (2009) Proceedings of the 4th International Workshop on Security, pp. 71-88
- McCullagh, N., Barreto, P.S.L.M., Efficient and forward-secure identity-based signcryption (2004) Cryptology EPrint Archive, Report 2004/117, , http://eprint.iacr.org/2004/117.pdf
- Boneh, D., Boyen, X., Short signatures without random oracles (2004) Advances in Cryptology - EUROCRYPT 2004, 3027 (2004), pp. 56-73

- Boneh, D., Boyen, X., Goh, E.-J., Hierarchical identity based encryption with constant size ciphertext (2005) Lecture Notes in Computer Science, 3494, pp. 440-456. , Advances in Cryptology - EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Proceedings
- Pointcheval, D., Stern, J., Security arguments for digital signatures and blind signatures (2000) Journal of Cryptology, 13, pp. 361-396
- http://crypto.stanford.edu/pbc/